Силабус навчальної дисципліни
«*МАТЕМАТИЧНІ ОСНОВИ КРИПТОЛОГІЇ*»

Спеціальність	*125 Кібербезпека*
Освітня програма	*125 Кібербезпека*
Освітній рівень	*Бакалавр*
Статус дисципліни	*Базова*
Мова викладання	*Українська*
Курс / семестр	*2 курс, 3 семестр*
Кількість кредитів ЄКТС	*5*
Розподіл за видами занять та годинами навчання	*Лекції – 24 год.*
	Практичні (семінарські) – …. год.
	Лабораторні – 24 год.
	Самостійна робота – 102 год.
Форма підсумкового контролю	*Залік*
Кафедра	*Кібербезпеки та інформаційних технологій, м. Харків, пр-т Науки 9-А, 057-702-18-31, http://www.kafcbit.hneu.edu.ua/*
Викладач (-і)	*Мілов Олександр Володимирович, к.т.н., проф.*
Контактна інформація викладача (-ів)	*oleksandr.milov@hneu.net*
Дні занять	*понеділок*
Консультації	*Понеділок 12.10; дистанційні; відповідно до графіку; індивідуальні*

Мета навчальної дисципліни "Математичні основи криптології" – ознайомлення з основами математичної теорії криптології; придбання навичок в практичному використанні, постановці і вирішенні задач шифрування інформації; розуміння суті інформаційних процесів в криптографічних системах; застосування комп'ютерів для вирішення завдань шифрування і дешифрування; розробка і використання математичних і обчислювальних моделей процесів шифрування інформації, їх оптимізація та вироблення напрямків вдосконалення.

Передумови для навчання

Інформатика за шкільною програмою, Математика за шкільною програмою / основи алгебри, операції над цілими числами, засоби обробки, передачі та відображення інформації, системи числення, простіші логічні операції над числами у двійковому форматі

Зміст навчальної дисципліни

Змістовій модуль 1. Традиційне шифрування

Тема 1. Вступ до криптології.
Тема 2. Модульна арифметика.
Тема 3. Матриці.
Тема 4. Традиційні шифри з симетричним ключем
Тема 5. Алгебраїчні структури.
Тема 6. Сучасні блокові шифри.

Змістовій модуль 2. Сучасні методи шифрування

Тема 7. Перетворення.
Тема 8. Застосування сучасних блокових шифрів.
Тема 9. Прості числа.
Тема 10. Квадратичне порівняння з модулем.
Тема 11. Криптографічна система RSA.
Тема 12. Криптосистема Рабина.

Матеріально-технічне (програмне) забезпечення дисципліни

Internet, MS Office

Сторінка курсу на платформі Moodle (персональна навчальна система) Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця за дисципліною «Математичні основи криптології» https://pns.hneu.edu.ua/course/view.php?id=5678	*Посилання:* 1. www.cyberpol.ru - Комп'ютерна злочинність і способи боротьби. 2. www.iso27000.ru - Інформаційний портал, присвячений питанням управління інформаційною безпекою. 3. www.itsec.ru - Інтернет-журнал «Інформаційна безпека». 4. www.inside-zi.ru - Інформаційно-методичний журнал «Захист інформації. Інсайд».

Рекомендовані джерела

Базова

1. В. Мао. Современная криптография: теория и практика. - СПб.: Вильямс, 2005, Д 85с.

2. Аграновский А. В., Хади Р. А. Практическая криптография: алгоритмы и их программирование - М.: СОЛОН-ПРЕСС, 2009

3. Бирюков А. А. Информационная безопасность: защита и нападение - М.: ДМК Пресс, 2012

Допоміжна література

4. *Вернет, Пэйн. Криптография. Официальное руководство RSA Security. - М.: Бином, 2002,342с.*
5. *Виега Д., Лебланк Д., Ховард М. 19 смертных грехов, угрожающих безопасности программ : Как не допустить типичных ошибок - М.: ДМК Пресс, 2009 v*
6. *Грэм, Кнут, Паташник. Конкретная математика. - М.: Мир, 1998, 145с.*
7. *П.Н. Девянин, О.О. Михальский, Д.И. Правиков, А.Ю. Щербаков. Программно-аппаратные средства обеспечения информационной безопасности. Теоретические основы компьютерной безопасности. - М.: Радио и связь, 2000, 176с.*
8. *А.А. Малюк, С.В. Пазизин, Н.С. Погожин. Введение в защиту информации в автоматизированных системах. - М.: Горячая Линия - Телеком, 2001, 126с.*
9. *А.А. Молдовян, Н.А. Молдовян, Гуц, Изотов. - Криптография: скоростные шифры. - СПб.: БХВ, 2002, 222 с.*
10. *Ноден, Ките. Алгебраическая алгоритмика. - М.: Мир, 1999, 192с.*

Система оцінювання результатів навчання

*Студента слід **вважати атестованим**, якщо сума балів, одержаних за результатами підсумкової/семестрової перевірки успішності, дорівнює або перевищує 60. Мінімально можлива кількість балів за поточний і модульний контроль упродовж семестру – 60 балів.*

Підсумкова оцінка з навчальної дисципліни розраховується з урахуванням балів, отриманих під час поточного контролю за накопичувальною системою. Сумарний результат у балах за семестр складає: "60 і більше балів – зараховано", "59 і менше балів – не зараховано" та заноситься у залікову "Відомість обліку успішності" навчальної дисципліни.

Більш детальна інформація щодо оцінювання наведена в технологічній карті дисципліни.

Накопичування рейтингових балів з навчальної дисципліни *(приклад)*

Види навчальної роботи	Мах кількість балів
Лекційні заняття	**12**

Виконання лабораторних робіт	**48**
Поточні КР	**40**
Максимальна кількість балів	**100**

Відповідність шкали оцінювання ЄКТС національній системі оцінювання та ХНЕУ ім. С. Кузнеця

Сума балів за всі види навчальної діяльності	Оцінка ЄКТС	Оцінка за національною шкалою	
		для екзамену (іспиту), диференційованого заліку, курсового проекту (роботи), практики, тренінгу	для заліку
90 – 100	A	відмінно	зараховано
82 – 89	B	добре	
74 – 81	C		
64 – 73	D	задовільно	
60 – 63	E		
35 – 59	FX	незадовільно	не зараховано
1 – 34	F		

Політики навчальної дисципліни

Політика дотримання академічної доброчесності,
Політика щодо пропусків занять,
Політика щодо виконання завдань пізніше встановленого терміну,
тощо

Більш детальну інформацію щодо компетентностей, результатів навчання, методів навчання, форм оцінювання, самостійної роботи наведено у Робочій програмі навчальної дисципліни «Математичні основи криптології», 2020.

Силабус затверджено на засіданні кафедри «31» серпня 2020 р. Протокол № 2